Безопасность устройств IOT в контексте изменения законодательства в области ИБ

Проблемы IOT

- Стремительный рост интереса и большое количество компаний, стремящихся заработать деньги в данной области
- Как следствие полное игнорирование нишевыми игроками вопросов ИБ
- Не понимание вопросов ИБ руководителями организаций, которые используют такие решения
- Вопросы хранения большого объема данны производителями
- Интеграция взаимодействия с интернето
- Физическая распределенность устройств

Проблемы IOT

CONFIG_*******_ROOT_PASSWORD=«sVGhNBRNyE57»

CONFIG_*******_ROOT_PASSWORD=«GFg7n0MfELfL»

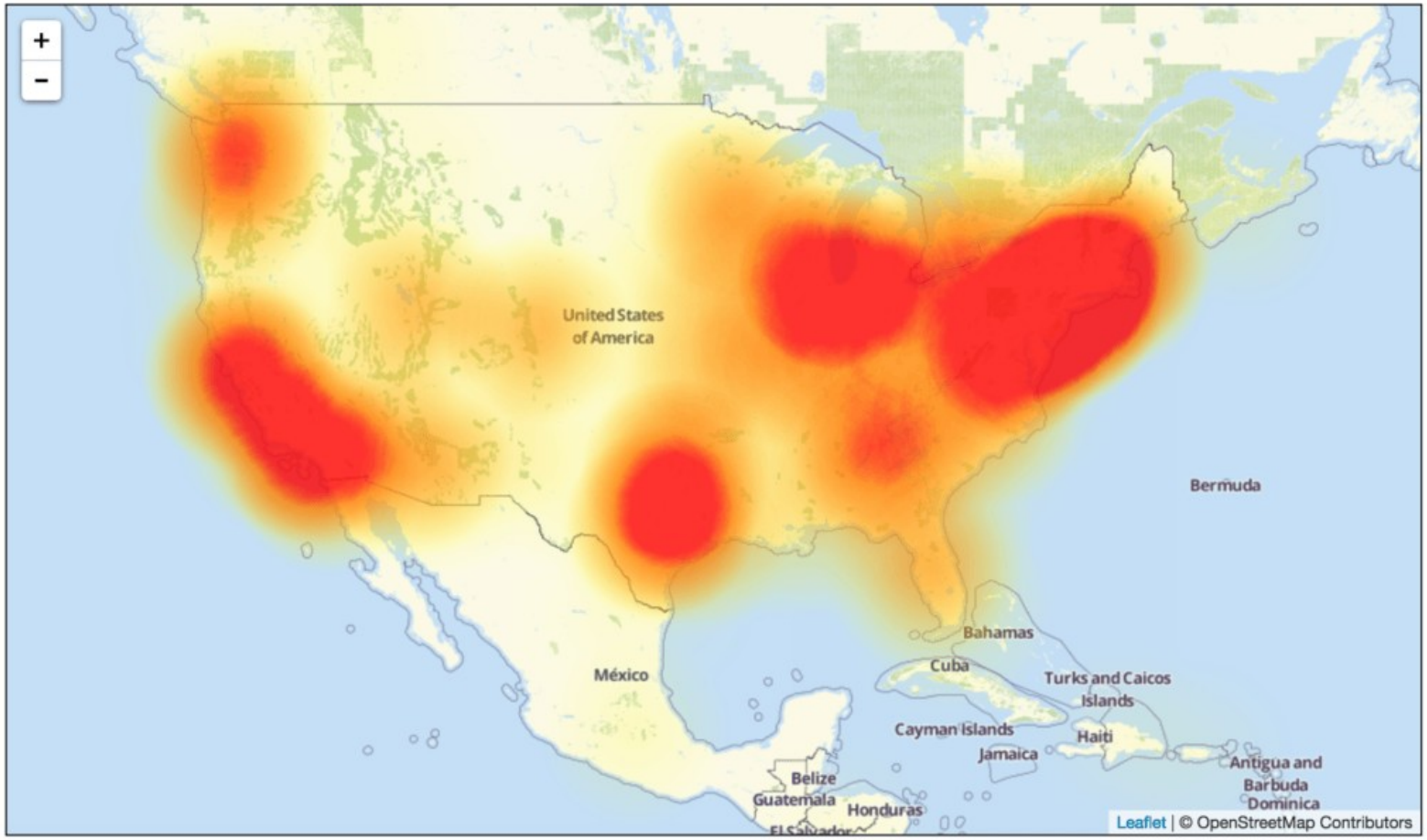
Пример уязвимости в камере в IP-камере

Проблемы IOT

DDOS атака мощностью 2 Тбита/сек на провайдера DNS Dyn в октябре 2016 г. с использованием ботнета Mirai, состоящего из зараженных IOT-устройств в результате был нарушен доступ к сайтам Twitter, Reddit, Github, Youtube

Ряд экспертов ИБ после этого выступили за регулирование отрасли

Проблемы IOT



Что есть у нас

В части законодательства:

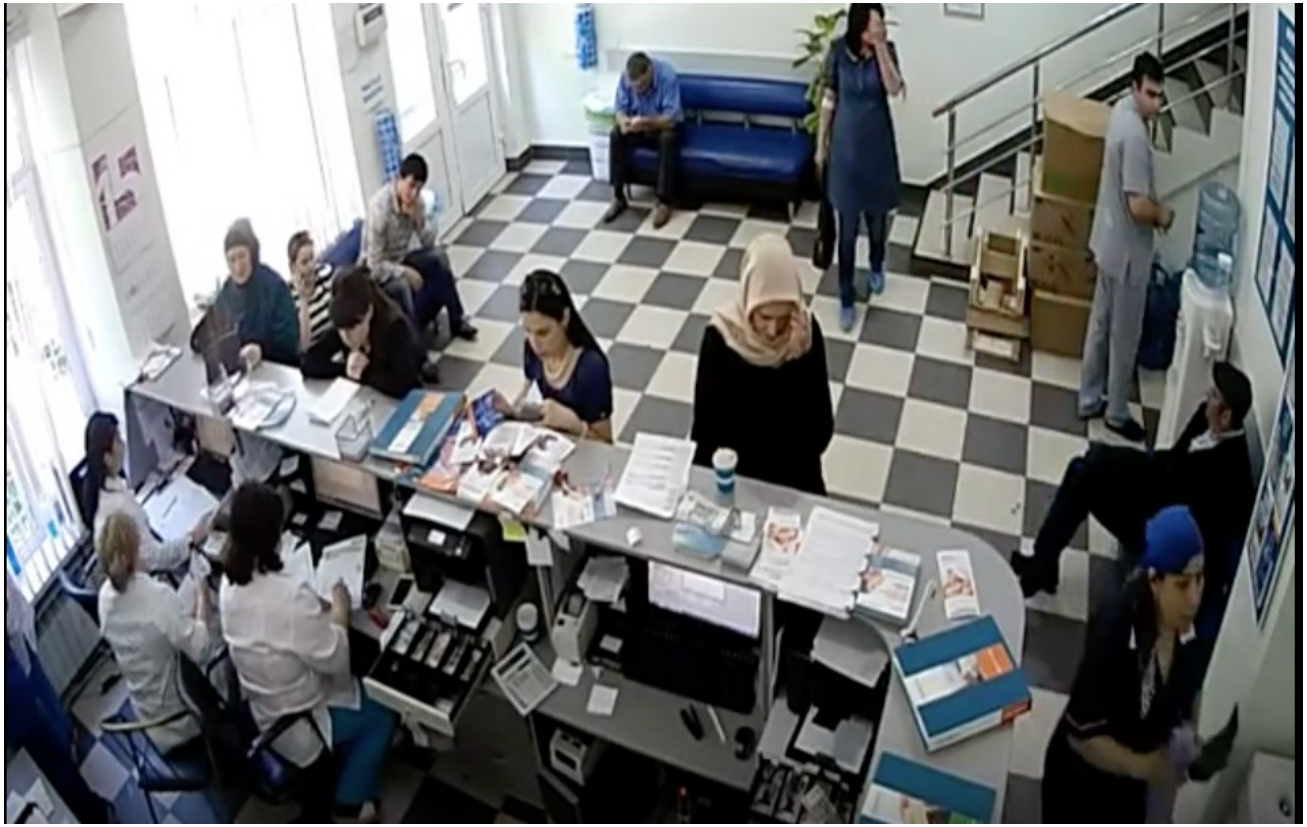
- Приказы регуляторов (ФСТЭК/ФСБ) по обеспечению безопасности персональных данных;

- ГОСТы по разным направлениям в области обеспечения ИБ

НО

В этих документах нет требований и мероприятий по безопасности IOT

Результат



Необходимо

-Разработать перечень мер нивелирующих риски IOT-устройств при подключении к интернету (и речь не про сертификацию);

- Правильно донести информацию до руководителей организаций и подразделений ИТ о необходимости обеспечения безопасности и реализации мер по защите IOT устройств при взаимодействии с интернетом

Приглашаем Вас к сотрудничеству!

www.infosystems.ru
Россия, 111123,
Москва ул. Плеханова, 4а
Тел: +7 (495) 120-04-02
E-mail: Info@infosystem.ru